IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of
Peyravian et al.

Serial No.: **09/458,410**

Filed: **December 10, 1999**

For: **Time Stamping Method Employing Multiple Receipts Linked by a Nonce**

Attorney's Docket No: **4541-004**

Patent Pending

Examiner: Aravind K. Moorthy

Group Art Unit: 2131

Confirmation No.: 8813

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☒ e-filed with the USPTO.

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) 273-8300.

June 30, 2006
Date

Kathleen Koppen

APPEAL BRIEF

This Appeal Brief is being timely filed within one month of the mailing date of the Notice of Panel Decision from the Pre-Appeal Brief Review dated June 7, 2006. As such, no extension of time fees should be due. The Commissioner is authorized to charge the requisite fee pursuant to 37 C.F.R. §41.20 and any additional fees required or due for entry of this Brief to IBM's Deposit Account No. 09/0461.

(1) REAL PARTY IN INTEREST

The real party in interest is IBM Corp., the assignee of the present invention.

(2) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences to the best of Applicants' knowledge.

(3) STATUS OF CLAIMS

A total of nineteen (19) claims numbered 1-19 have been presented for examination, all of which are pending. The Examiner has finally rejected claims 1-19. Accordingly, Applicant appeals the final rejection of claims 1-19.

(4) STATUS OF AMENDMENTS

All amendments have been entered to the best of Applicants' knowledge.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

The claimed invention relates to a protocol for time stamping digital documents received at a Trusted Outside Agency (TSA) so that a date of the document may be verified. *Spec.*, p. 4, ll. 2-3.

As seen in Figure 1, the TSA receives data that identifies a document (e.g., a hash value generated on the document), and creates a two-part time stamp receipt. Specifically, the TSA generates a random linking value and concatenates the received identifying data with the linking value to create the first part of the time stamp receipt. The TSA then concatenates a time indication with the linking value to generate the second part of the time stamp receipt. The time indication indicates when the TSA received the identifying data. Once both parts of the time stamp receipt have been created, the TSA separately signs both parts of the receipt using, for example, the TSA's private key, and transmits one or both parts of the signed time stamp receipt to the requestor. *Spec.*, p. 6, ln. 4 – p. 7, ln. 12.

In the event a dispute arises concerning the document, the two-part time stamp receipt may be used to prove the existence of the document as of the date the TSA received the

identifying data. To verify the disputed document, the first and second parts of the signed time stamp receipt are verified using the TSA's public verification key. The identifying data included in the first part of the time stamp receipt is compared to the disputed document. For example, if the identifying data in the first part of the time stamp receipt comprises a hash value generated on the document, the disputed document is also hashed. Provided these two hash values are equal, the linking value in the first part of the time stamp receipt is compared against the linking value in the second part of the time stamp receipt. The time that the TSA received the identifying data is verified if the linking value in the first part of the time stamp receipt matches the linking value in the second part of the time stamp receipt. This time is considered to be the priority date of the document. *Spec.*, p. 7, ln. 12 – p. 8, ln. 2.

(6) GROUNDS OF REJECTION

The Examiner finally rejected claims 1-19 under 35 U.S.C. §102(b) as being anticipated by WO 92/03000 to Haber (hereinafter "Haber").

The Examiner also rejected claims 1-19 under 35 U.S.C. §112 ¶¶1-2 alleging that the specification fails to enable the claims, and that the claims are indefinite because they do not particularly point out and distinctly claim the subject matter Applicants' regard as their invention.

The Examiner also rejected claims 1 and 9 under §101 alleging that the claims recite a use without setting forth any steps involved in the process.

(7) ARGUMENTS RELATING TO THE REJECTIONS

A. Haber fails to anticipate claim 1 under 35 U.S.C. §102(b).

The issue regarding claim 1 is whether Haber creates the claimed two-part time stamp receipt. Each of the first and second parts of the receipt must include a value that links the two parts together, and each being created during the same time stamping transaction. For the reasons set forth below, Haber does not disclose this limitation of claim 1.

It is well settled that, under 35 U.S.C. §102, every element or limitation of a claim must identically appear in a single prior art reference for that reference to anticipate the claim. *In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990). Further, anticipation requires that the single prior art reference disclose every element of the claimed invention arranged in the same manner as claimed. *Lindemann Maschinenfabrik v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1458 (Fed. Cir. 1984).

Claim 1 is directed to a method of time stamping a digital document that allows the existence of the document as of a particular date to be verified. Claim 1 recites that an outside agency creates first and second different time stamp receipts. The first receipt includes data identifying a document received by an outside agency (e.g., a hash) and the second includes a time indication that indicates when the agency received the identifying data. Both parts of the time stamp receipt include a linking value that links the parts together. Thus, both the first and second receipts time stamp the same document and are created during the same time-stamping transaction. For reference, claim 1 appears below in its entirety.

> 1. A method for time-stamping a digital document comprising:
> receiving identifying data derived from a document at an outside agency;
> creating at said outside agency a first receipt based on said identifying data;
> creating at said outside agency a second receipt, different from said first receipt, based on a time indication that indicates when the document was received at the outside agency;
> inserting a linking value into said first and second receipts that links the identifying data in the first receipt with the time indication in the second receipt;
> certifying said first and second receipts at said outside agency using a cryptographic signature scheme.

Haber discloses a method of creating a time-stamp receipt that may be used to verify the existence of a document as of a particular date. However, rather than creating two different parts of a time stamp receipt related to the same document, the method of Haber creates a single receipt associated with a single transaction for a single document. Haber then concatenates that single receipt with another previously created time-stamp receipt. Notably,

however, this previously created time-stamp receipt is created in Haber during a completely different and unrelated transaction.

More particularly, each time stamp receipt created in Haber contains a hash (H_k) of a document (D_k), the ID of the author (ID_k), a sequential receipt number (r_k), and a time indication (t_k) that indicates when the TSA processed the receipt. *Haber*, p. 14, ln. 10 – p. 15, ln. 1. Thus, each single receipt for a given document D_k in Haber contains *both* the identifying data *and* a time indication. The Examiner asserts that Haber creates the claimed two-part receipts; however, this assertion is non-sensical in the context of the Haber. Indeed, there is no need for Haber to create a second time stamp receipt to include information (i.e., the time indication) already contained in the first receipt.

Nevertheless, the Examiner cites pages 16-17 to support the assertion that Haber creates a two-part receipt. Scrutiny reveals that this section only contradicts the Examiner's assertion. Haber explicitly discloses that the TSA adds (i.e., concatenates) the data of a previously created receipt D_{k-1} to the current receipt D_k. After adding this data, the receipt created for D_k contains both its own time t_k and the time t_{k-1} of the previously created receipt. *Haber*, p. 16, ll. 3-5. This time indication t_{k-1} does not indicate a time that the TSA received the document D_k as is required by the claims. Contrastingly, it t_{k-1} indicates the time that the TSA time stamped an earlier unrelated document D_{k-1}. That is, time stamping document D_{k-1} is a different transaction performed on a different document at a different time, and thus, the time indication t_{k-1} is independent of the document D_k currently being processed. It cannot indicate the time that the TSA received document D_k as is required by the claims.

Further, Haber necessarily fails to disclose the claimed linking value. The claimed linking value links the first receipt containing the identifying data with the second receipt containing the time that the outside agency received the identifying data. Haber, in contrast, simply creates a composite receipt representing the current transaction and all prior transactions. *Haber*, p. 21, ll. 3-7. According to Haber, the agency creating the time stamp

receipt creates a single, composite certificate that includes a composite hash of "the entire history of the TSA time-stamping operation" concatenated with the current transaction. *Haber*, pg. 21, ll. 14-17 (emphasis added). There is no linking value in Haber as required by the claimed invention. Moreover, there is no need for a linking value when each composite receipt created by the TSA includes a composite hash of all prior receipts ever created by the TSA.

Applicants note that the Examiner has admitted in earlier Office Actions that another patent to Haber failed to disclose the claimed linking value. Particularly, the currently cited Haber patent '000 claims priority from two U.S. applications, which have since issued as U.S. Patent Nos. 5,136,646 and 5,136,647. In previous Office Actions, the Examiner cited Haber RE 34,954, which is a reissue of the '647 patent. The '646 and '647 patents disclose slightly different methods of forming the time-stamp receipts -- i.e., the '646 patent creates the composite receipt described above, while the '647 patent concatenates previous and current receipts. However, both the '646 and '647 patents create the receipts to include both the data and a time indication in a single receipt. Applicants successfully overcame this RE 34,954-based §102 rejection thereby forcing the Examiner to withdraw the rejection and admit, "Haber is silent in expressly disclosing inserting a linking value into said first and second receipts that links the identifying data in the first receipt with the time indication in the second receipt." *Office Action dated July 2, 2004*, p. 3, 14-16 (emphasis added). Given this explicit admission, it is surprising that the Examiner now refuses to consider Applicants' remarks regarding this failure of Haber. Indeed, the Examiner's prior statement is a *de facto* admission that Haber fails to anticipate claim 1.

Haber does not create the requisite first and second receipts, nor does Haber disclose the claimed linking value. Because Haber fails to teach each and every element of independent claim 1, the §102 rejection necessarily fails as a matter of law.

B. Haber fails to anticipate claim 9 under 35 U.S.C. §102(b).

Claim 9 is directed to a method wherein a requestor transmits identifying data derived from a document to the outside agency for time stamping. The outside agency creates the two-part time stamp receipt, cryptographically signs both parts of the time stamp receipt, and returns both parts to the requestor. For reference, claim 9 appears below in its entirety.

> 9. A method for time-stamping a digital document comprising:
> transmitting identifying data derived from said document to an outside agency;
> receiving from said outside agency a first receipt signed by said outside agency using a cryptographic signature scheme, said first receipt including a first digital sequence generated based on said identifying data;
> receiving from said outside agency a second receipt signed by said outside agency using a cryptographic signature scheme, said second receipt being different from said first receipt and containing a second digital sequence based on a time indication that indicates when the document was received at the outside agency; and
> wherein said first and second receipts comprise a linking value that links the identifying data in the first receipt with said time indication in the second receipt.

As with claim 1, the first part of the time stamp receipt includes the identifying data sent to the outside agency by the requestor, and the second part includes a time indication that indicates when the outside agency received the identifying data. Both parts of the time stamp receipt include a linking value that links the two parts together.

For reasons similar to those stated above, Haber does not create the requisite two-part time stamp receipt. Therefore, whatever the requestor May receive from the TSA in Haber is not the first and second parts of a two-part time stamp receipt, each of which includes a linking value. Accordingly, Haber also fails to anticipate claim 9 under §102.

C. The 35 U.S.C. §112 ¶¶1-2 rejections are based on a fundamentally flawed assertion and must be withdrawn.

The Examiner also rejected claims 1-19 under 35 U.S.C. §112 ¶1 and ¶2. The Examiner asserts that the specification fails to support, "receiving identifying data derived from a

document at an outside agency." Guided by this assertion, the Examiner then postulates that claims 1 and 9 recite a use without setting forth any positive steps delineating how the process is actually practiced. *Final Office Action*, p. 3, ¶6. These assertions, and thus, the rejections themselves, are based on the misguided belief that the specification fails to support: 1) that the outside agency of the claims receives the identifying data; and 2) that the identifying data is derived from a document.[1] However, the §112 rejections are without merit and should be withdrawn.

The specification explicitly states, "[t]he hash value H generated on document D or a selected portion thereof is transmitted to and received by the TSA at step 104." *Spec*, p. 6, lines 4-5; Figure 1 (emphasis added). Moreover, page 9 of the specification, lines 3-11, describe that a user's computer could hash and transmit the data to a server application executing on a computer at the outside agency. One skilled in the art would easily understand that such transmissions could occur over a communication network such as the Internet, for example. Thus, the specification unquestionably supports the fact that the outside agency receives the identifying data, and further makes clear that a computer at the outside agency could receive the identifying data from another computer over a network. The technical expertise required to transmit and receive digital data is well-known, and need not be described in explicit detail by the specification.

Further, pages 4 and 5 of the specification and Figure 1 describe one embodiment where a hash function takes a document D (or selected portions thereof) as input, and computes a hash value H from that document. Because the hash value (i.e., output) is generated on the document content (i.e., input), the hash value is necessarily derived from the document. These passages and the figure prove that the specification supports the claimed

[1] The undersigned agent telephoned the Examiner on or about February 22, 2006 to clarify the reasons for the §112 and §101 rejections. The Examiner stated that both the §112 and the §101 rejections were based on the belief that the specification did not support or explain how the identifying data was "derived" from a document.

subject matter, and provides reasonable, explicit examples of how one skilled in the art might "derive" identifying data from the document. No one skilled in the art armed with the specification and drawings would need to perform any experimentation – let alone undue experimentation - to practice the claimed invention. The §112 rejections should be withdrawn.

D. The 35 U.S.C. §101 rejection is based on a fundamentally flawed assertion and must be withdrawn.

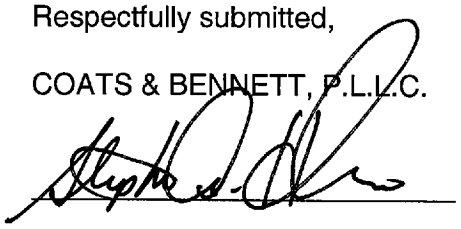
Regarding the §101 rejection, the Examiner's stated position is that the claims recite a use without setting forth any steps involved in the process. *Final Office Action*, p. 3, ¶7. During the telephone conversation of February 22, 2005, the Examiner stated that the §101 rejection was based on the belief that the specification did not support or explain how the identifying data was derived from the document, and thus, the §101 rejection is related to the §112 ¶1 rejection discussed above. However, as previously noted, this "lack of support" assertion is unfounded. Applicants have adequately described "how" the claimed invention is used, and therefore, has necessarily described "what" that invention is. The claims accurately reflect what Applicants consider their invention. Therefore, Applicant has complied with the requirements of both §112 and §101. The §101 rejection is based on a fundamentally flawed theory and should be withdrawn.

Conclusion

For the reasons set forth above, Haber fails to anticipate claims any of the claims 1-19 under §102 and must be withdrawn. Further, because the specification and the figure fully support all claimed subject matter, both the §112 and the §101 rejections are flawed and must be withdrawn. Accordingly, all claims 1-19 being appealed herein are patentable over the cited art, and the Board is respectfully requested to overturn all rejections.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.



Dated: June 30, 2006

Stephen A. Herrera
Registration No.: 47,642
Telephone: (919) 854-1844

(8) CLAIMS APPENDIX

1. A method for time-stamping a digital document comprising:

receiving identifying data derived from a document at an outside agency;

creating at said outside agency a first receipt based on said identifying data;

creating at said outside agency a second receipt, different from said first receipt, based on a time indication that indicates when the document was received at the outside agency;

inserting a linking value into said first and second receipts that links the identifying data in the first receipt with the time indication in the second receipt;

certifying said first and second receipts at said outside agency using a cryptographic signature scheme.

2. The time-stamping method of claim 1 wherein said identifying data comprises a digital representation of at least a portion of said document.

3. The time-stamping method of claim 2 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

4. The time-stamping method of claim 3 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

5. The time-stamping method of claim 1 wherein said first receipt comprises at least a portion of said identifying data and a nonce.

6. The time-stamping method of claim 1 wherein said first receipt comprises a digital sequence generated by applying a pre-determined function to said identifying data.

7. The time-stamping method of claim 1 wherein one of said first and second receipts comprises a user identification number associated with a user.

8. The time-stamping method of claim 7 wherein one of said first and second receipts comprises a sequential record number.

9. A method for time-stamping a digital document comprising:

transmitting identifying data derived from said document to an outside agency;

receiving from said outside agency a first receipt signed by said outside agency using a cryptographic signature scheme, said first receipt including a first digital sequence generated based on said identifying data;

receiving from said outside agency a second receipt signed by said outside agency using a cryptographic signature scheme, said second receipt being different from said first receipt and containing a second digital sequence based on a time indication that indicates when the document was received at the outside agency; and

wherein said first and second receipts comprise a linking value that links the identifying data in the first receipt with said time indication in the second receipt.

10. The time-stamping method of claim 9 wherein said identifying data comprises a digital representation of at least a portion of said document.

11. The time-stamping method of claim 10 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.

12. The time-stamping method of claim 11 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.

13. The time-stamping method of claim 9 wherein said first receipt comprises at least a portion of said identifying data and a nonce.

14. The time-stamping method of claim 9 wherein said first receipt comprises a digital sequence generated by applying a pre-determined function to said identifying data.

15. The time-stamping method of claim 9 wherein one of said first and second receipts comprises a user identification number associated with a user.

16. The time-stamping method of claim 15 wherein one of said first and second receipts comprises a sequential record number.

17. The time-stamping method of claim 9 wherein a common cryptographic signature scheme is used to sign both said first and second receipts.

18. The time-stamping method of claim 9 wherein different cryptographic signature schemes are used to sign said first and second receipts.

19. The time-stamping method of claim 9 wherein said linking value is a nonce value.

(9) EVIDENCE APPENDIX

There is no further evidence not contained in the prosecution history.

(10) RELATED PROCEEDINGS APPENDIX

There are no related proceedings.